ARCHITECTURE FOR SECURE NETWORK VOICE

Michael S. McBeth
Space and Naval Warfare Systems Center, Charleston
Communications System Department
Yorktown, Virginia

Raymond Cole, Jr.
Naval Research Laboratory
Information Technology Division
Washington, D.C.

R. Brian Adamson
Newlink Global Engineering, Inc.
Springfield, Virginia

***Abstract*¾ Voice over Internet Protocol (VoIP is an emerging technology that promises economic and performance advantages by reducing hardware and enabling object oriented voice applications. Technology and products alone will not automatically bring these advantages to the military. A system architecture approach is needed. Our approach translates user driven requirements into products that are secure, interoperable, and easy to use. Using the DoD's C4ISR Architecture Framework, Version 2.0, we define operational, system, and technical views for secure Network voice. From these views, we explore some enabling technologies and applications to make Network voice an Information Appliance for Joint Vision 2010.**

INTRODUCTION

ADVANCES in high speed networks, processing, capability and Internet telephony are fueling a drive to bring Network voice to the warfighter. The military needs an architecture to structure Network voice solutions so they fuse voice and data over DoD backbone networks, provide access to legacy and emerging voice services, and position the military to take advantage of advanced knowledge-based voice applications.

Since 1995, researchers at the Naval Research Laboratory have been experimenting with Network voice using a tool called Interactive VOice eXchange (IVOX)[1][2]. Through this prototyping effort, we have learned about problem areas in Network voice. These lessons drive home the need for a system architecture.

C4ISR ARCHITECTURE FRAMEWORK FOR SECURE NETWORK VOICE

Operational, system, and technical views provide a uniform way of describing information systems [3][4]. Fig. 1 shows our high level operational concept. In this figure, Network voice extends from ships at sea to expeditionary forces ashore to airborne aircraft to Command centers to peacekeeping and disaster relief forces.

Network voice glues legacy systems together **and** provides new ways of linking voice circuits with combat direction activities.

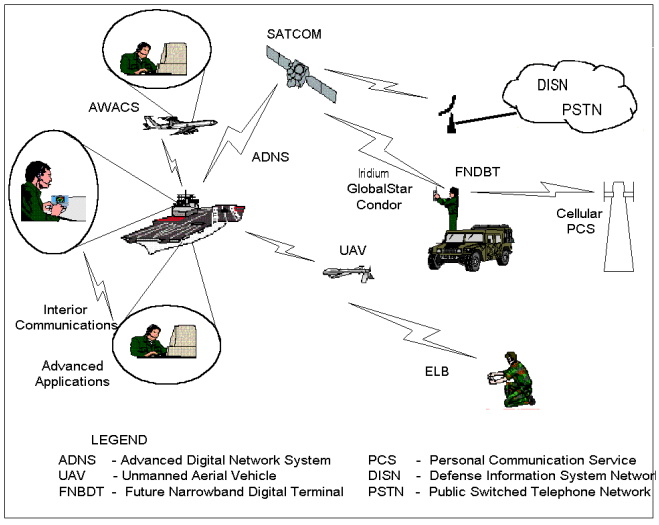

Fig. 1. High level operational concept graphic for secure Network voice.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Architecture for Secure Network Voice	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Research Laboratory,Information Technology Division,4555 Overlook Avenue, SW,Washington,DC,20375**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**4**	

Fig. 2 shows how enabling technologies couple desired voice services—both past and future—to our target architecture.

Legacy voice services include Plain Old Telephone Service (POTS), the Defense Red Switched Network (DSRN), and secure tactical voice nets like those found in the U.S. Navy's Single Audio System (SAS).

Fortunately, today's computer telephony marketplace provides the building blocks for creating Interworking Function (IWF) gateways. These gateways let Network voice users talk with their legacy equipped counterparts.

Our team is developing a prototype gateway based on IVOX for the Extended Littoral Battlespace (ELB) Advanced Concept Technology Demonstration (ACTD). Users will be able to make telephone calls and talk on tactical radio voice nets using the ELB gateway [5].

Interoperability with emerging secure voice services including Iridium™ and GlobalStar™ satellite-based handsets and Integrated Services Digital Network (ISDN)-based Secure Terminal Equipment (STE) phones will be accomplished using the National Security Agency's Future

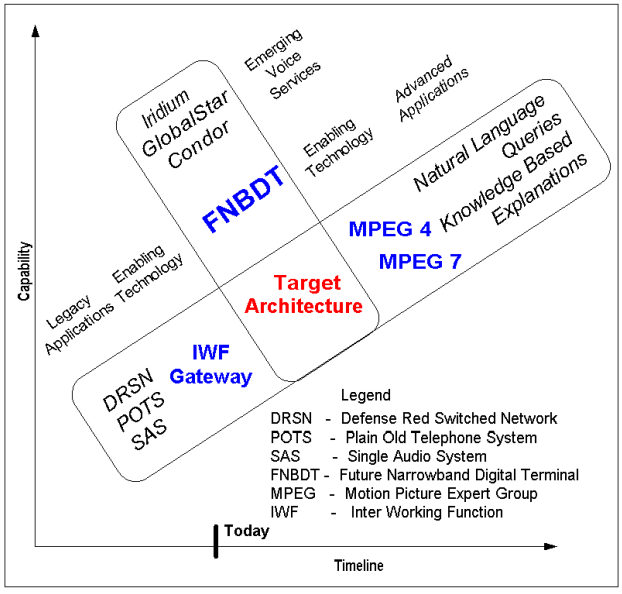

Fig. 2. How enabling technologies couple desired applications to the target architecture.

Narrowband Digital Terminal (FNBDT) signaling protocol [6].

The FNBDT, pronounced "Fend-Bit," protocol provides a Network-independent overlay for interoperation between secure voice systems.

However, FNBDT is more than an overlay, it's a "prescription for interoperability." The FNBDT signaling plan is structured to provide the core functions needed to setup a secure call, exchange capabilities, negotiate session parameters, change modes during a call, and terminate a call.

The architects of the FNBDT signaling plan standardized core functions for all FNBDT capable equipment. They left room for specialized capabilities and emerging services to be added as appendices to the signaling plan.

The security aspects of the proposed architecture are being built around this concept and we are working on FNBDT appendices for Network voice and MPEG 4 applications to be used with the overlay.

Although FNBDT provides a solid foundation for building security into a Network voice architecture, there is more to security than an interoperable signaling protocol.

BUILDING SECURITY INTO A SECURE NETWORK VOICE ARCHITECTURE

Several hard-learned lessons regarding security and cryptographic communications demand attention when considering alternative approaches for a secure Network voice architecture. First among these is that "security is only as good as the weakest link in the chain." This means that no matter how robust the architecture, system implementations will always be at risk for security flaws. Good system design is the surest way to avoid security flaws and achieve a usable product [7].

Accurate threat models play a key role in understanding the real risks a system faces and the corresponding security measures needed to protect it.

Defining threat models for the far-reaching concept shown in Fig. 1 is problematic. First, the geographic range for Network voice applications extends from calls confined inside a ship to calls with forward forces operating in hostile territory. Second, the timeline for Network voice appears to be open-ended and security measures defined today will be subject to attacks by adversaries using tomorrow's technology.

One approach we considered is to tailor the security protections to the Defense in Depth framework shown in Fig.3. Defense in Depth forces adversaries to compromise several protections to reach systems or information. With this approach the strength of protection measures for Network voice applications can be decreased and simplified for calls within a protected enclave (zones 1, 2, & 3). However, voice applications need to be "path aware" to insure calls are adequately protected. So the simplicity gained by simplified protection measures could be offset by the complexity of path awareness. Defense in Depth is constantly evolving as new threats emerge and security technologies improve. Network voice applications that depend on these security features may not work when they change. The Defense in Depth approach lacks the flexibility of true end-to-end protection measures.

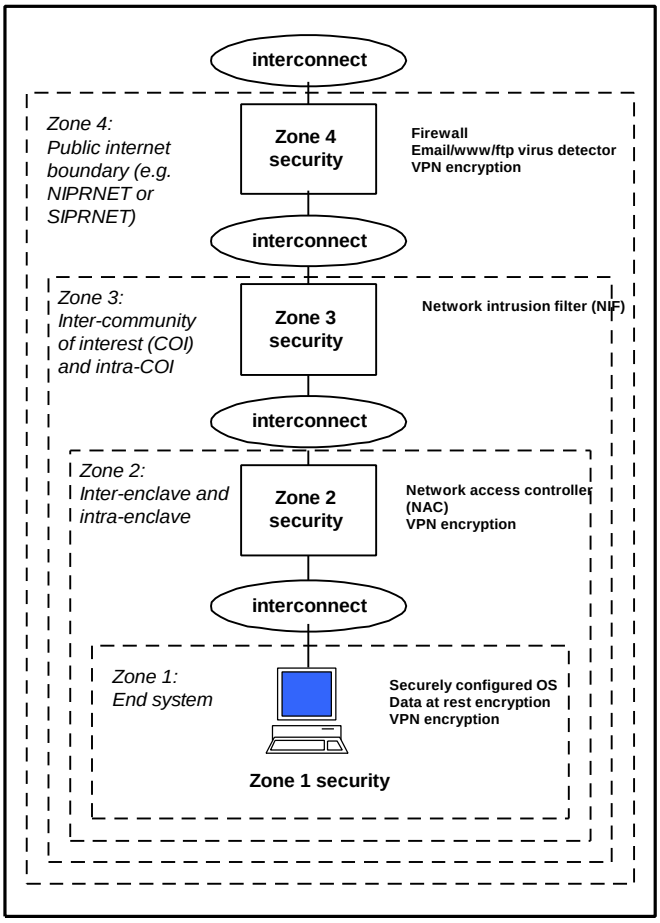

Fig. 3. Defense in Depth Framework.

Our favored approach is to decouple the security architecture from the Defense in Depth framework and strive for a "heterogeneous" security approach that focuses on end-to-end encryption independent of the underlying Network. Network voice security becomes yet another layer within the Defense in Depth framework. With this approach the strength of protection measures for Network voice applications is independent of the path that calls take within the Network. The price for this independence is having to deal with key management and encryption for all secure calls even when they are confined within a protected enclave.

Security and interoperability of Network Voice with legacy and emerging voice services are important issues, but it's the future of Network voice that offers a never-before-seen shift in services available to users [8].

ADVANCED APPLICATIONS BASED ON MPEG-4 AND MPEG-7

Imagine following a tactical operation on a computer display in a Command center. You move the display cursor over to a track representing one of your aircraft and "hook" the contact by clicking on it. Instantly, a tactical radio window appears on your display and you hear voice from an associated radio net through your headphones.

Associating Network voice streams with objects in advanced combat decision systems is a new capability and it suggests possibilities for easing operator workload and increasing "Speed of Command."

The Motion Picture Experts Group (MPEG) provides a family of open standards for multimedia including MPEG-4 and MPEG-7. These standards will enable advanced

applications through their object orientation, multi-rate scaling, and interactive features [9].

Table 1 outlines some advantages of MPEG-4 that apply to Network voice. These capabilities offer opportunities for crafting solutions that push the evolution of voice data into knowledge.

Table 1. Advantages of MPEG-4

- Based on Open Standards
- Provides hooks to proprietary management & protection—you can build military grade encryption into it
- Supports advanced "interactive" audio visual applications
- Tools include uniform and high quality audio & video encoding
- Scalable content (multi-rate) encoding and low bit-rate streams for mobile & wireless
- Includes MPEG-2 AAC for multichannel surround sound
- Can be coupled with a "synthetic face" for a computer generated decision aid
- MPEG-J (Dec 99) Subset of JAVA for building platform independent information appliances

.

FUTURE WORK

We plan to continue refining the target architecture as we learn new lessons from the ELB gateway project and establish the next generation operational requirements

REFERENCES

[1] Brian Adamson and Joe Macker, "IVOX - The Interactive Voice eXchange Application," MILCOM 96 Conference Proceedings, 1996.

[2] Michael S. McBeth, R. Brian Adamson, and Raymond Cole, Jr, "Application of Network Voice to Navy and DoD Telecommunications," MILCOM 98 Conference Proceedings, 1998.

[3] P. Kathie Sowell, "A Framework for Optimizing the Utility of Architectures—DoD's Strategic Direction." MILCOM 98 Conference Proceedings, 1998.

[4] C4ISR Architecture Framework, Version 2.0, C4ISR Architecture Working Group, 18 December 1997.

[5] R. Brian Adamson, Tom Moran, Raymond Cole, Jr., and Michael S. McBeth, "Extended Littoral Battlespace (ELB) Secure Network Voice Gateway," MILCOM 1999 Conference Proceedings, 1999.

[6] Future Narrowband Digital Terminal Signaling Plan, FNBDT-210, Revision 1.0, National Security Agency, 04 December 1998.

[7] Bruce Schneier, "Why Cryptography Is Harder Than It Looks," The Se-Com Project, Montgomery Research, Inc., San Francisco, CA.

[8] Christos A. Polyzois et al., "From POTS to PANS: A Commentary on the evolution to Internet Telephony," IEEE Internet Computing Magazine, May/June 1999.

[9] Bob Koenen, "MPEG-4 Multimedia for Our Time," IEEE Spectrum Magazine, February 1999.